(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2004 (18.03.2004)

PCT

(10) International Publication Number
WO 2004/023730 A2

(51) International Patent Classification[7]: H04L 12/28

(21) International Application Number:
PCT/US2003/027644

(22) International Filing Date:
4 September 2003 (04.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/236633 6 September 2002 (06.09.2002) US

(71) Applicant: CAPITAL ONE FINANCIAL CORPORATION [US/US]; 2980 Fairview Park Drive, Falls Church, VA 22042 (US).

(72) Inventors: GRIFFITH, Terry, A.; 12421 Stone Horse Court, Glen Allen, VA 23059 (US). MORAN, Stephen, M.; 11105 Mill Place Court, Glen Allen, VA 23060 (US). BRAGG, John, M.; 14105 Waters Edge Circle, Midlothian, VA 23112 (US).

(74) Agent: JOHNSON, Jay, B.; Baker Botts L.L.P., 2001 Ross Avenue, Suite 600, Dallas, TX 75201 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR REMOTELY MONITORING WIRLESS NETWORKS

(57) Abstract: A system for monitoring a wireless network is provided. The system includes a security network including a plurality of monitoring devices coupled to a centralized security manager. The security network is operable to manage access to a data network associated with a plurality of authorized devices. Each monitoring device is operable to receive packets communicated from one or more wireless device and communicate one or more of the packets to the centralized security manager. Each packet is associated with a communication session. The centralized security manager is operable to receive and analyze the one or more packets communicated from each monitoring device. The centralized security manager is further operable to determine whether a particular communication session is valid based on the analysis of at least one particular packet associated with a particular wireless device, and to communicate an alert if the particular communication session is not valid.

WO 2004/023730 A2

access to the wireless LAN. In addition, if the attacker can sniff the wireless traffic, he may also be able to inject false traffic into the network. Thus, the attacker may be able to issue commands on behalf of the authorized user by injecting traffic into the network and hijacking the authorized user's session. Using this technique, the attacker may trick the network into passing sensitive data from the backbone of the network to the attacker's wireless station. The attacker may thus gain access to sensitive data that normally would not be sent over the wireless LAN.

Another security risk of using wireless LANs involves unauthorized devices being placed on the wireless LAN. For example, an internal employee wanting to add his own wireless capabilities to a wired network may plug his own base station or access point into the wired network. This may create a security risk if the added access point has not been properly configured, as attackers may gain access to the network through the unauthorized access point. Alternatively, an attacker may physically place a base station or access point on the network providing the attacker remote access to the network using wireless communications.

is operable to manage access to a data network associated with a plurality of authorized devices. Each monitoring device is operable to receive packets communicated from one or more wireless device and select one or more of the received packets to be analyzed. Each packet is associated with a communication session. Each monitoring device is further operable to determine whether the selected packets are to be analyzed locally or by the centralized security manager. Each monitoring device is further operable to communicate the selected packets to the centralized security manager if it is determined that the selected packets are to be analyzed by the centralized security manager. Each monitoring device is further operable to analyze the selected packets if it is determined that the selected packets are to be analyzed locally, and to determine whether the communication session is valid based on the analysis of the selected packets. The centralized security manager is operable to receive the selected packets from the monitoring device if it is determined that the selected packets are to be analyzed by the centralized security manager, analyze the received selected packets, and determine whether the communication session is valid based on the analysis of the received selected packets.

According to yet another embodiment, a method of validating a communications session in a wireless network is provided. The method includes receiving one or more packets communicated from a wireless device at a monitoring devices operable to monitor at least a portion of a network including a plurality of authorized devices. The one or more packets are associated with a communication session. The method further includes determining whether the communication session is valid, which includes determining the manufacturer of the wireless device based on the one or more packets, determining whether the manufacturer of the wireless device matches the manufacturer of at least one of the plurality of authorized wireless clients, determining whether the wired equivalency privacy (WEP) associated with the wireless device is turned on, and determining whether the MAC address of the wireless device matches the MAC address of any of the plurality of authorized wireless devices.

turned on, determining whether the SSID of the wireless access point matches the SSID of the authorized access points, determining whether the BSS MAC address of the wireless access point matches the BSS MAC address of one of the authorized access points, and determining whether the wireless access point is broadcasting.

Still another advantage is that the local wireless monitors may also be operable to analyze packets to detect unauthorized communication sessions, such as in a situation in which a connection to the centralized security manager is not currently available. The centralized security manager as well as each wireless monitor may have a database of authorized communication sessions, access points, and wireless clients. The centralized security manager may communicate with each wireless monitor to keep their respective database updated or synchronized.

Other technical advantages will be readily apparent to one having ordinary skill in the art from the following figures, descriptions, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and for further features and advantages, reference is now made to the following description, taken in conjunction with the accompanying drawings, in which:

FIGURE 1 illustrates a system for remotely monitoring wireless networks in accordance with an embodiment of the present invention;

FIGURE 2 illustrates an example wireless monitor in accordance with an embodiment of the present invention;

FIGURE 3 illustrates an example centralized security manager in accordance with an embodiment of the present invention;

FIGURE 4 is a top view of a floor in a building, illustrating an example configuration of a portion of wireless LAN and a campus security network in accordance with an embodiment of the present invention;

FIGURE 5 illustrates a method of monitoring communication sessions in a wireless network, such as a wireless LAN, in accordance with an embodiment of the present invention;

network 12. Data network 12 may be any network in which data may be communicated and may in particular embodiments include a plurality of campuses 16 connected to a communications network 18. Each campus 16 may include one or more local area networks (LANs), metropolitan area networks (MANs), wide area networks (WANs), portions of the internet, or any other appropriate wireline, optical, wireless, or other links.

In the embodiment shown in FIGURE 1, one particular campus 16 includes a wireless LAN 20 having a two-level hierarchical topology. In this embodiment, wireless LAN 20 includes a plurality of authorized wireless base stations, or access points, 22 connected to a campus backbone network 24. Authorized access points 22 may include any device capable of receiving and/or transmitting wireless communications. Each authorized wireless access point 22 provides a number of authorized mobile stations, or clients, 26 a point of access to data network 12. Thus, authorized clients 26 may communicate with authorized access points 22 using wireless communications to gain access to data network 12. Authorized clients 26 may include personal computers (PCs), laptops, handheld devices such as personal digital assistants (PDAs), or any other device capable of transmitting and/or receiving wireless communications.

The number of authorized clients 26 connected to data network 12 through each authorized access point 22 may vary over time as authorized clients 26 initiate, establish, and terminate communication sessions with data network 12. In some embodiments, each authorized client 26 may gain access to data network 12 through any authorized access point associated with wireless LAN 20.

Campus backbone network 24 may include any network suitable to communicate with authorized access points 22. In some embodiments, campus backbone network 24 comprises a wired local area network (LAN) based on any of a variety of protocols, such as Ethernet, token ring, or fiber distributed data interface (FDDI) protocols, and including any of a variety of topologies, such as bus, ring, star, or tree topologies, for example. As discussed above, campus backbone network 24 may be connected to communications network 18 such that the particular campus 16 may communicate with the other campuses 16. Communications network 18 may

However, as discussed below in greater detail, security network 14 is operable to identify rogue access points 36 and act accordingly to reduce or eliminate their potential security risks.

In addition to unauthorized access points, unauthorized clients pose a threat to security. For example, as shown in FIGURE 1, an attacker with an unauthorized client 38 (such as a laptop or PDA, for example) may attempt to access data network 12 through one or more authorized access points 22. For example, if the area of coverage of an authorized access point 22 located within a building extends outside of the building, an attacker located outside the building but within the area of coverage may attempt to access data network 12 through the authorized access point 22 using the unauthorized client 38. For example, an attacker may be able to detect, or "sniff," security information, such as password information or security key information, from wireless signals being communicated between the authorized access point 22 and authorized clients 26. The attacker may then be able to use the security information to masquerade as an authorized client 26 in order to access data network 12 through the authorized access point 22. The attacker may also be able to inject false traffic from the unauthorized client 38 into data network 12 via the authorized access point 22 in order to hijack an authorized communication session. In addition, the attacker may use an arpspoof technique to trick data network 12 into passing sensitive data to unauthorized client 38 that would not ordinarily be sent over a wireless link. However, as discussed below in greater detail, security network 14 is operable to identify unauthorized clients 38 and to act accordingly to reduce or eliminate their potential security risks.

Thus, security network 14 is generally operable to provide security to data network 12 by reducing or eliminating the security risks associated with rogue access points 36 and unauthorized clients 38. In some embodiments, security network 14 is operable to monitor wireless communications associated with wireless LANs 20 and to identify invalid or unauthorized communication sessions (in other words, communications sessions involving a rogue access point 36 and/or an unauthorized client 38), and to prevent such invalid or unauthorized communication sessions.

communication session associated with wireless LAN 20. For example, the packet may have been communicated by an authorized or unauthorized client 26 or 38 and may concern a request by the client 26 or 38 to establish a communication session with a particular authorized or rogue access point 22 or 36. As another example, the packet have been broadcast from an authorized or rogue access point 22 or 36 and intended for one or more authorized or unauthorized clients 26 or 38. As another example, the packet may have been communicated from an authorized or rogue access point 22 or 36 in response to a communication received from an authorized or unauthorized client 26 or 38. The term "packet" is intended to include any group or bundle of data, such as a datagram, frame, message, segment, or cell, for example, which may be transmitted by any one or more types of communications media, such as wireline, optical, wireless, or any other type of communications links.

Packet filtering module 62 may be operable to filter packets collected by packet sniffing module 60 to determine relevant, or interesting, packets. Interesting packets may include packets concerning the authentication, authorization, and/or establishment of a communication session, such as packets communicated by authorized and rogue access points 22 and 36 and/or authorized and unauthorized clients 26 and 38 during key exchange handshaking, for example. In some embodiments, relevant or interesting packets selected by packet filtering module 62 generally do not include traffic data packets communicated after a communication session is established. In a particular embodiment, packet filtering module 62 may select as relevant or interesting based on whether particular types of encryption are turned on or off on the wireless device from which particular packets were received.

Packet routing module 64 may be operable to determine whether particular selected as relevant or interesting by packet filtering module 62 are to be analyzed locally by the packet analysis module 66 of the wireless monitor 32 or communicated to and analyzed by centralized security manager 30. In particular embodiments, this determination comprises determining whether a connection between the particular wireless monitor 32 and centralized security manager 30 is available such that the wireless monitor 32 may communicate the interesting packets to centralized security manager 30 for analysis. A connection to centralized security manager 30 may not be

Countermeasure module 70 may be operable to initiate or direct a countermeasure in response to an invalid or unauthorized communication session determined by packet analysis module 66. For example, if an unauthorized client 38 is identified, countermeasure module 70 may be operable to disassociate the unauthorized client 38 from all authorized access points 22 associated with wireless LAN, thus preventing the unauthorized client 38 from gaining access to the data network 12 through any authorized access points 22. As another example, countermeasure module 70 may redirect unauthorized client 38 to a honey pot which may trick unauthorized client 38 into believing that unauthorized client 38 is progressing through the actual data network 12. This technique may be used to keep unauthorized client 38 connected long enough to contact security personnel or law enforcement and/or to detect the methods of attack used by unauthorized client 38 in order to deter or prevent future attacks. In particular embodiments, countermeasure module 70 is operable to initiate or direct such countermeasures in response to commands received from appropriate security personnel. In other embodiments, countermeasure module 70 may be operable to automatically initiate or direct such countermeasures (in other words, without direction from security personnel) if an invalid or unauthorized communication session is identified.

Session database 72 may store a record of one or more authorized and/or or unauthorized communications sessions associated with wireless LAN 20 or data network 12. In addition, wireless monitor 32 may communicate such records to centralized security manager 30. For example, in a situation in which particular interesting packets are analyzed locally because a communication link to send the packets to centralized security manager 30 is not currently available, packet analysis module 66 may identify authorized communication sessions, generate records regarding each identified authorized session, and store the records session database 72. Wireless monitor 32 may later communicate records stored in session database 72 to centralized security manager 30 after the connection between the wireless monitor 32 and centralized security manager 30 has been restored. In addition, centralized security manager 30 may send records to session database 72 at particular times such that session database 72 may be updated.

may first determine whether the communication session with which the interesting packet is associated is a new communication session or an already established communication session, then determine whether the packet was originally communicated from a wireless client (such as an authorized or unauthorized client 26 or 38) or from a wireless access point (such as an authorized or rogue access point 22 or 36), and then determine whether the communication session is a valid or authorized session based on further analysis of the packet.

To determine whether the communication session is a new communication session or an already established communication session, packet analysis module 82 may first determine whether the packet is a data packet or a beacon packets. A beacon packet may be a packet communicated in a beacon broadcast by a wireless access point or client, such as a beacon broadcast by a wireless client searching for an wireless access point with which to communicate. Data packets may include packets communicated by a wireless access point or client in any manner other than a beacon broadcast. After determining whether the packet is a data packet or a beacon packet, packet analysis module 82 may then determine which portions of the packet are interesting and split the packet to extract the interesting portions. Packet analysis module 82 may then format the extracted interesting portions such that the interesting portions may be properly analyzed. Packet analysis module 82 may then compare the formatted interesting portions with a database of information to determine whether the communication session with which the interesting packet is associated is a new communication session or an already established communication session. In particular embodiments, packet analysis module 82 may then compare the formatted interesting portions with a beacon packet information database if the packet is a beacon packet and a data packet information database if the packet is a data packet.

In some embodiments, centralized security manager 30 is generally operable to prevent the establishment of unauthorized communication sessions in real time. Thus, centralized security manager 30 may not be concerned with packets associated with communication sessions identified as established communication sessions by packet analysis module 82. Thus, if packet analysis module 82 determines that the communication session discussed above is an established communication session,

of the wireless client does not match the manufacturer of any authorized client 26, packet analysis module 82 may determine that the wireless client is an unauthorized client 38 and that the communications session is thus invalid or unauthorized.

Packet analysis module 82 may also determine whether one or more particular security measures are turned on or off. For example, packet analysis module 82 may determine whether the wired equivalent privacy (WEP) associated with the wireless client is turned on or off. Packet analysis module 82 may be operable to determine whether the WEP is turned on or off based on a particular bit in the packet header. In particular embodiments, if packet analysis module 82 determines that the WEP is turned off, packet analysis module 82 may determine that the wireless client is an unauthorized client 38 and that the communications session is thus invalid or unauthorized.

In particular embodiments, packet analysis module 82 may also determine whether the MAC address of the wireless client matches the MAC address of any of the authorized clients 26. For example, authorized device database 88 may include a list of the MAC address for each authorized client 26, and packet analysis module 82 may compare the MAC address of the wireless client with the list. If the MAC address of the wireless client does not match the MAC address of any authorized client 26, packet analysis module 82 may determine that the wireless client is an unauthorized client 38 and that the communications session is thus invalid or unauthorized.

Thus, regarding packets originally communicated from a wireless client, packet analysis module 82 may determine whether a communication session is valid or authorized based at least on one or more of the determinations discussed above, namely, whether the manufacturer of the wireless device matches the manufacturer of any of the authorized clients 26, whether the WEP associated with the wireless client is turned on, and whether the MAC address of the wireless device matches the MAC address of any of the authorized clients 26. In a particular embodiment, packet analysis module 82 may determine that a particular communication session is valid or authorized only if the manufacturer of the wireless client matches the manufacturer of at least one authorized client 26, the WEP associated with the wireless client is turned

wireless access point with the list. If the BSS MAC address of the wireless access point does not match the BSS MAC address of any authorized access point 22, packet analysis module 82 may determine that the wireless access point is an unauthorized access point 36 and that the communications session is thus invalid or unauthorized.

In addition, packet analysis module 82 is also operable to determine whether the wireless access point is broadcasting. In particular embodiments, authorized access points 22 are configured to respond to communications received from wireless devices, but to not broadcast signals. In such embodiments, if packet analysis module 82 determines that the wireless access point is broadcasting signals, packet analysis module 82 may determine that the wireless access point is an unauthorized access point 36 and that the communications session is thus invalid or unauthorized.

Thus, regarding packets originally communicated from a wireless access point, packet analysis module 82 may determine whether a communication session is valid or authorized based at least on one or more of the determinations discussed above, namely, whether the manufacturer of the wireless device matches the manufacturer of any of the authorized access points 22, whether the WEP associated with the wireless access point is turned on, whether the SSID of the wireless device matches the SSID of the authorized access points 22, whether the BSS MAC address of the wireless device matches the MAC address of any of the authorized access points 22, and whether the wireless access point is broadcasting signals. In a particular embodiment, packet analysis module 82 may determine that a particular communication session is valid or authorized only if the manufacturer of the wireless access point matches the manufacturer of at least one authorized access point 22, the WEP associated with the wireless access point is turned on, the SSID of the wireless access point matches the SSID of the authorized access points 22, the MAC address of the wireless access point matches the MAC address of one of the authorized access points 22, and the wireless access point is not broadcasting.

It should be understood that packet analysis module 66 of each wireless monitor 32 may be operable to perform one, some, or all of the functions operable to be performed by packet analysis module 82 of centralized security manager 30. For example, each wireless monitor 32 may include similar or identical software as

FIGURE 4 is a top view of a floor in an office building, illustrating an example configuration of at least a portion of wireless LAN 20 and campus security network 28. A plurality of authorized access points 22 connected to campus backbone network 18 are geographically dispersed to create a particular area of coverage to support wireless communications with authorized mobile clients 26. The area of coverage 52 of each authorized access point 22 may depend on a variety of factors, such as the characteristics of the particular authorized access point 22, the location of the authorized access point 22 within building 50, and the presence of physical structures which may obstruct wireless communications in the vicinity of the authorized access point 22, for example. The area of coverage 52 of each authorized access point 22 may also extend in a vertical direction, and may thus provide coverage for more than one floor of building 50. As shown in FIGURE 4, the area of coverage 52 of particular authorized access points 22 may extend beyond one or more outer walls of building 50, thus potentially providing authorized and unauthorized clients 26 and 38 access to data network 12 through such authorized access points 22. For example, as shown in FIGURE 4, an unauthorized client 38a may be located outside of building 50 but within the area of coverage 52 of a particular authorized access point 54 of the authorized access points 22, and thus able to communicate with the particular authorized access point 54. Thus, unauthorized mobile client 38a may attempt to access data network 12 via authorized access point 54 while remaining outside building 50.

In addition, one or more rogue access points 36 may also be connected to campus backbone network 18. As discussed above with reference to FIGURE 1, rogue access points 36 may be connected to campus backbone network 24 by internal employees desiring mobile access to data network 12 or by an outside attacker desiring access to data network 12. Rogue access points 36 may also include access points that were authorized to be connected to campus backbone network 24, but are misconfigured in some way. The area of coverage 52 of a rogue access point 36 may extend outside building 50, thus potentially providing authorized and unauthorized clients 26 and 38 access to data network 12 through the rogue access point 36. For example, as shown in FIGURE 4, an unauthorized client 38b may be located outside

(such as authorized mobile clients 26). The one or more packets of information may be associated with a communication session, as discussed above with reference to FIGURE 2.

At step 202, the monitoring device may filter the one or more received packets to select a relevant, or interesting, packet. For example, interesting packets may include packets concerning the authentication, authorization, and/or establishment of a communication session, such as packets communicated during key exchange handshaking, for example.

At step 204, it is determined whether a connection between the monitoring device and a centralized security manager is available such that the monitoring device may communicate the interesting packet to the centralized security manager for analysis. If it is determined at step 204 that a connection between the monitoring device and the centralized security manager is not available, the monitoring device may analyze the interesting packet locally at step 206 to determine whether the communication session with which the interesting packet is associated is valid or authorized. Alternatively, if it is determined at step 204 that a connection with the centralized security manager is available, the interesting packet is sent from the monitoring device to the centralized security manager at step 208. For example, in the embodiment shown in FIGURE 1, the interesting packet may be communicated from the monitoring device to the centralized security manager via communications network 18.

At step 210, the interesting packet is logged into a packet database associated with the centralized security manager. At step 212, the centralized security manager may determine whether the communication session with which the interesting packet is associated is a new session or an established session. This decision is described in greater detail below with reference to FIGURE 6. If it is determined that the communication session is an established session, no action is taken by the centralized security manager at step 214. However, if it is determined that the communication session is a new session, the centralized security manager determines whether the new session is valid or authorized at step 216. This determination is described in greater detail below with reference to FIGURE 7.

broadcast by a wireless access point or client, such as a probe frame transmitted by a wireless client in search of a wireless access point.

If it is determined that the packet is a data packet, the packet may be split at step 232 to extract interesting portions of the packet. The interesting portions of the packet may then be formatted at step 234 such that the interesting portions may be properly analyzed. At step 236, the formatted interesting portions may be compared with a database of data packet information to determine whether the communication session with which the data packet is associated is a new communication session or an already established communication session.

Similarly, if it is determined that the packet is a beacon packet, the packet may be split at step 238 to extract interesting portions of the packet. The interesting portions of the packet may then be formatted at step 240 and compared with a database of beacon packet information at step 242 to determine whether the communication session with which the beacon packet is associated is a new communication session or an already established communication session.

FIGURE 7 illustrates a method of determining whether a communication session with which an interesting packet is associated is valid or authorized, as described above regarding step 216 of FIGURE 5. At step 250, it may be determined whether the packet was originally communicated from a wireless client (such as an authorized or unauthorized client 26 or 38) or from a wireless access point (such as an authorized or rogue access point 22 or 36). In particular embodiments, this determination may include analyzing one or more bits in the packet that are turned on or off depending on whether the packet was communicated from a wireless client or a wireless access point. In one embodiment, the determination includes analyzing a portion of the MAC address associated with the packet.

If it is determined at step 250 that the packet was communicated from a wireless client, the packet may be further analyzed at steps 252 through 256 to determine whether the communication session is valid or authorized. Alternatively, if it is determined at step 250 that the packet was communicated from a wireless access point, the packet may be further analyzed at steps 258 through 266 to determine whether the communication session is valid or authorized.

wireless access point matches the manufacturer of any authorized access point, such as described above regarding step 252. At step 260, it may be determined whether one or more particular security measures are turned on or off, such as described above regarding step 254. At step 262, it may be determined whether the SSID of the wireless access point matches the SSID of one or more authorized access points. At step 264, it may be determined whether the BSS MAC address of the wireless access point matches the BSS MAC address of one or more authorized access points This may include comparing the BSS MAC address of the wireless access point with a list of the BSS MAC address for each authorized access point. If the BSS MAC address of the wireless access point does not match the BSS MAC address of any authorized access point, it may be determined that the wireless access point is an unauthorized access point and that the communications session is thus unauthorized.

At step 266, whether the wireless access point is broadcasting may be determined. In particular embodiments, authorized access points are configured to not broadcast signals. Thus, in such embodiments, if it is determined that the wireless access point is broadcasting signals, it may be determined that the wireless access point is an unauthorized access point and that the communications session is thus unauthorized.

Thus, as shown in FIGURE 7, it may be determined that the wireless access point is an authorized access point and that the communications session is thus authorized if the manufacturer of the wireless access point matches the manufacturer of at least one authorized access point, the WEP associated with the wireless access point is turned on, the SSID of the wireless access point matches the SSID of the authorized access points, the BSS MAC address of the wireless access point matches the BSS MAC address of one of the authorized access points, and the wireless access point is not broadcasting signals.

FIGURE 8 illustrates a method of analyzing an interesting packet locally at a wireless monitor to determine whether a communication session associated with the packet is valid or authorized, as described above regarding step 206 of FIGURE 5. For example, as described above regarding step 204 of FIGURE 5, an interesting

session being established. If a connection with the centralized security manager is not available at step 296, the monitoring device may wait at step 300 until a connection becomes available in order to pass the relevant records to the centralized security manager. The monitoring device and the centralized security manager may communicate with each other to keep their respective database updated or synchronized.

Although an embodiment of the invention and its advantages are described in detail, a person skilled in the art could make various alterations, additions, and omissions without departing from the spirit and scope of the present invention as defined by the appended claims.

4. The system of Claim 1, wherein:

the plurality of authorized devices includes a plurality of authorized wireless access points and a plurality of authorized wireless clients, each of the wireless access points operable to provide one or more of the authorized wireless clients access to the data network; and

the centralized security manager further comprises a countermeasure module operable to prevent the wireless device access to the data network via each of the plurality of wireless access points if the wireless device is not one of the plurality of authorized devices.

5. The system of Claim 1, wherein the centralized security manager further comprises a countermeasure module operable to direct the wireless device to a honey pot if the particular wireless device is not one of the plurality of authorized devices.

6. The system of Claim 1, wherein the centralized security manager further comprises a countermeasure module operable to update a session database based on the determination of whether the particular communication session is valid.

7. The system of Claim 1, wherein:

the plurality of authorized devices includes a plurality of wireless access points and a plurality of authorized wireless clients, each of the wireless access points operable to provide one or more of the authorized wireless clients access to the data network;

the packet analysis module of the centralized security manager is further operable to determine whether the particular wireless device is a wireless access point or a wireless client based on the analysis of the at least one particular packet; and

the packet analysis module of the centralized security manager is operable to determine whether the particular wireless device is one of the plurality of authorized devices by:

12. The system of Claim 7, wherein the packet analysis module of the centralized security manager is operable to determine whether the wireless access point is one of the plurality of authorized wireless access points at least by determining whether the wired equivalency privacy (WEP) associated with the wireless access point is turned on.

13. The system of Claim 7, wherein the packet analysis module of the centralized security manager is operable to determine whether the wireless access point is one of the plurality of authorized wireless access points at least by determining whether the MAC address of the wireless access point matches the MAC address of any of the plurality of authorized wireless access points.

14. The system of Claim 7, wherein the packet analysis module of the centralized security manager is operable to determine whether the wireless access point is one of the plurality of authorized wireless access points at least by determining whether the service set identifier (SSID) of the wireless access point matches the service set identifier of each of the plurality of authorized wireless access points.

15.

16. The system of Claim 7, wherein the packet analysis module of the centralized security manager is operable to determine whether the wireless access point is one of the plurality of authorized wireless access points at least by determining whether the wireless access point is broadcasting packets.

22. The method of Claim 17, further comprising updating a session database associated with the centralized security manager based on the determination of whether the communication session is valid.

23. The method of Claim 17, wherein the plurality of authorized devices includes a plurality of wireless access points and a plurality of authorized wireless clients, each of the wireless access points operable to provide one or more of the authorized wireless clients access to the data network; and wherein the method further comprises:

determining whether the wireless device is a wireless access point or a wireless client based on the analysis of the at least one data packet; and

wherein determining whether the communication session is valid comprises:

if the wireless device is a wireless access point, determining whether the wireless access point is one of the plurality of authorized wireless access points; and

if the wireless device is a wireless client, determining whether the wireless client is one of the plurality of authorized wireless clients .

24. The method of Claim 23, wherein determining whether the wireless client is one of the plurality of authorized wireless clients comprises:

determining the manufacturer of the wireless client; and

determining whether the manufacturer of the wireless client matches the manufacturer of at least one of the plurality of authorized wireless clients.

25. The method of Claim 23, wherein determining whether the wireless client is one of the plurality of authorized wireless clients comprises determining whether the wired equivalency privacy (WEP) associated with the wireless client is turned on.

32. A system for monitoring a wireless network, comprising:

a security network including a plurality of monitoring devices coupled to a centralized security manager, the security network operable to manage access to a data network associated with a plurality of authorized devices;

wherein each monitoring device comprises:

a packet sniffing module operable to receive packets communicated from one or more wireless device; and

a packet routing module operable to communicate one or more of the packets to the centralized security manager; and

wherein the centralized security manager comprises

a packet collection module operable to receive the one or more packets communicated from each monitoring device;

a packet analysis module operable to:

analyze the one or more packets; and

determine based on the analysis of at least one particular packet associated with a particular wireless device whether the particular wireless device is one of the plurality of authorized devices; and

an alert module operable to communicate an alert if the particular wireless device is not one of the plurality of authorized devices.

34. A method of monitoring a wireless network, comprising:

receiving one or more packets communicated from a wireless device at one of a plurality of monitoring devices operable to monitor at least a portion of a network comprising a plurality of authorized wireless access points and a plurality of authorized wireless clients;

communicating at least one particular packet of the one or more packets to a centralized manager coupled to each of the plurality of monitoring devices;

analyzing the at least one particular packet;

determining whether the wireless device is one of the plurality of authorized devices based on the analysis of the at least one particular packet; and

communicating an alert if the wireless device is not one of the plurality of authorized devices.

35. The method of Claim 34, further comprising:

determining whether the wireless device is a wireless access point or a wireless client based on the analysis of the at least one data packet; and

wherein determining whether the wireless device is one of the plurality of authorized devices comprises:

if the wireless device is a wireless access point, determining whether the wireless access point is one of the plurality of authorized wireless access points; and

if the wireless device is a wireless client, determining whether the wireless client is one of the plurality of authorized wireless clients .

37. The system of Claim 36, wherein:

each monitoring device further comprises a local session database operable to store a record regarding a particular communication session if the monitoring device determines whether or not the particular communication session is valid; and

the centralized security manager is further operable to update a central session database based on the determination of whether the particular communication session is valid.

38. The system of Claim 36, wherein the packet routing module is operable to determine whether selected packets are to be analyzed by the monitoring device or by the centralized manager by determining whether a connection is available for communicating the selected packets from the monitoring device to the centralized manager.

39. The system of Claim 36, wherein each monitoring device further comprises an local alert module operable to:

communicate an alert if it is determined by the monitoring device that the communication session is not valid;

store a record of the alert communicated from the monitoring device; and

communicate the record of the alert to the centralized security manager.

40. The system of Claim 36, wherein each monitoring device further comprises an local alert module operable to:

store a record regarding the communication session if it is determined by the monitoring device that the communication session is valid; and

communicate the record regarding the communication session to the centralized security manager; and

wherein the centralized security manager is further operable to update a central session database based on the record regarding the communication session.

44. The method of Claim 41, further comprising:

communicating an alert from the monitoring device if it is determined by the monitoring device that the communication session is not valid;

storing a record of the alert communicated from the monitoring device; and

communicating the record of the alert to the centralized security manager.

45. The method of Claim 41, further comprising:

storing a record regarding the communication session if it is determined by the monitoring device that the communication session is valid;

communicating the record regarding the communication session to the centralized security manager; and

updating a session database associated with the centralized security manager based on the record regarding the communication session.

49. Software for monitoring a wireless network, the software being embodied in computer-readable media and when executed operable to:

receive one or more packets communicated from a wireless device, the one or more packets associated with a communication session;

determine whether the communication session is valid, including:

determining the manufacturer of the wireless device based on the one or more packets;

determining whether the manufacturer of the wireless device matches the manufacturer of at least one of the plurality of authorized wireless clients;

determining whether the wired equivalency privacy (WEP) associated with the wireless device is turned on; and

determining whether the MAC address of the wireless device matches the MAC address of any of the plurality of authorized wireless devices.

50. The software of Claim 49, wherein determining whether the communication session is valid further comprises determining whether the service set identifier (SSID) of the wireless device matches the service set identifier of each of the plurality of authorized wireless devices.

51. The software of Claim 49, wherein determining whether the communication session is valid further comprises determining whether the wireless device is broadcasting packets.

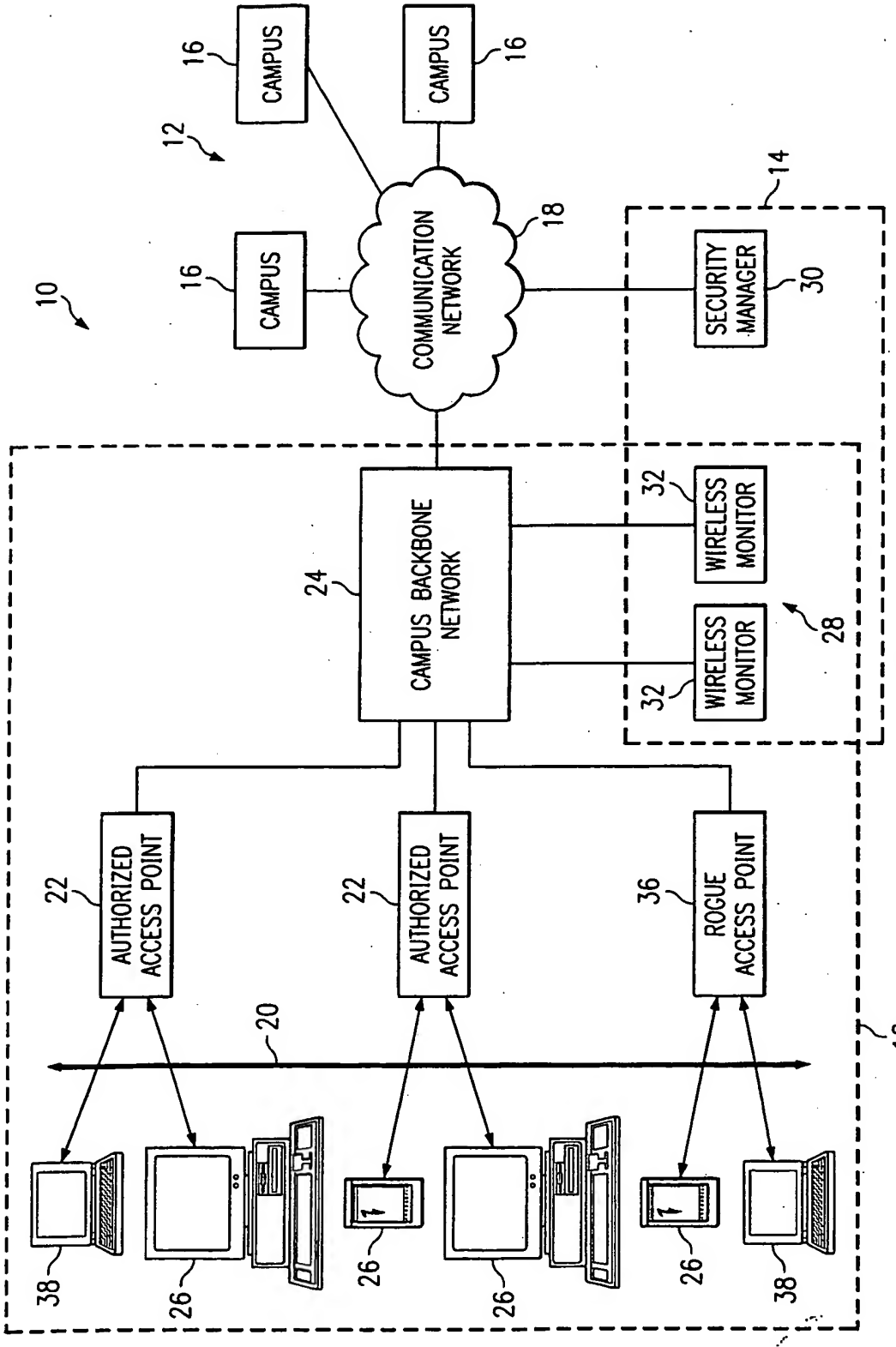

10
12
14
16
CAMPUS
CAMPUS
CAMPUS
CAMPUS
18
COMMUNICATION NETWORK
SECURITY MANAGER
30
24
CAMPUS BACKBONE NETWORK
32
WIRELESS MONITOR
32
WIRELESS MONITOR
28
22
AUTHORIZED ACCESS POINT
22
AUTHORIZED ACCESS POINT
36
ROGUE ACCESS POINT
20
16
38
26
26
26
38

FIG. 1

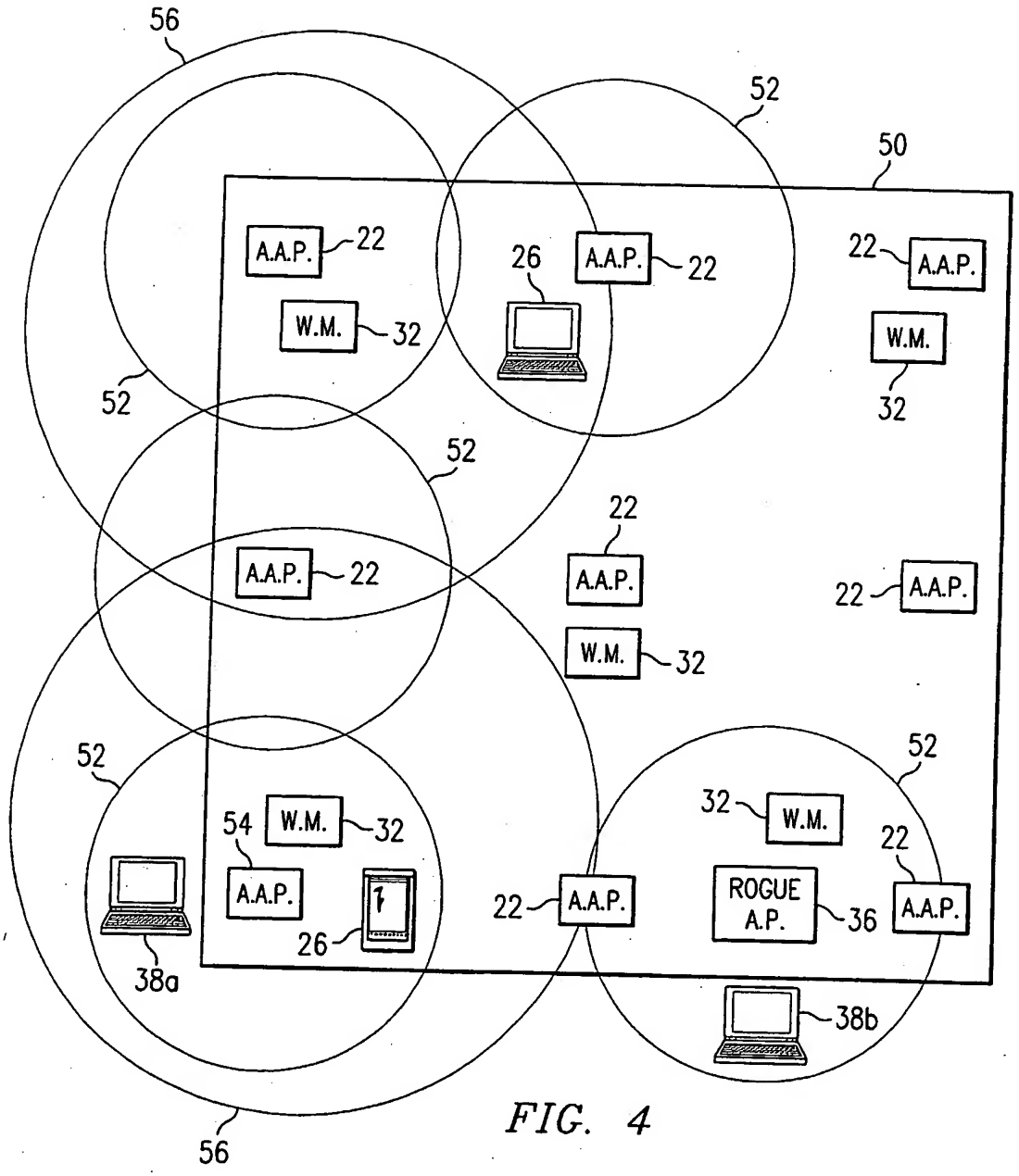
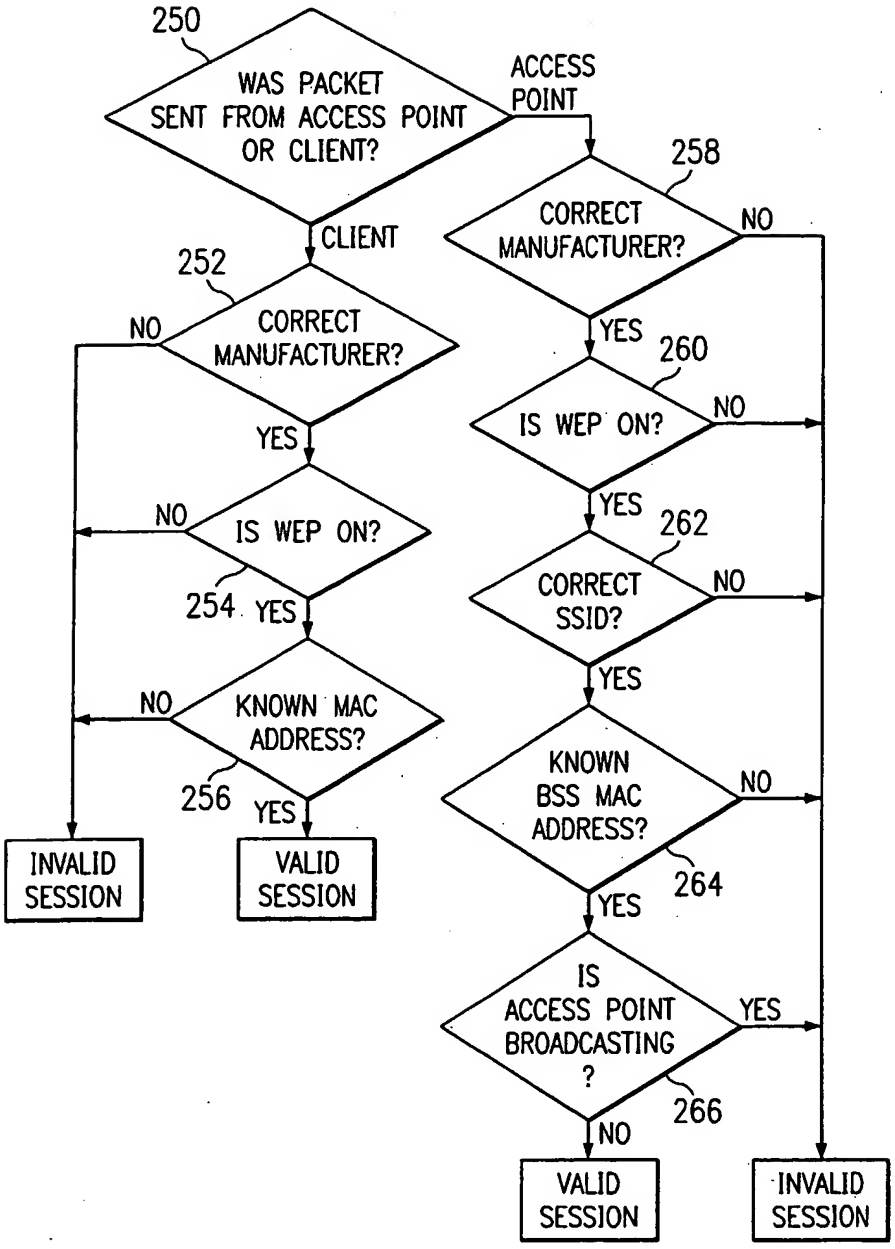


FIG. 4

FIG. 7



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2004 (18.03.2004)

PCT

(10) International Publication Number
WO 2004/023730 A3

(51) International Patent Classification[7]: H04L 12/28

(21) International Application Number:
PCT/US2003/027644

(22) International Filing Date:
4 September 2003 (04.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/236633 6 September 2002 (06.09.2002) US

(71) Applicant: CAPITAL ONE FINANCIAL CORPORATION [US/US]; 2980 Fairview Park Drive, Falls Church, VA 22042 (US).

(72) Inventors: GRIFFITH, Terry, A.; 12421 Stone Horse Court, Glen Allen, VA 23059 (US). MORAN, Stephen, M.; 11105 Mill Place Court, Glen Allen, VA 23060 (US). BRAGG, John, M.; 14105 Waters Edge Circle, Midlothian, VA 23112 (US).

(74) Agent: JOHNSON, Jay, B.; Baker Botts L.L.P., 2001 Ross Avenue, Suite 600, Dallas, TX 75201 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

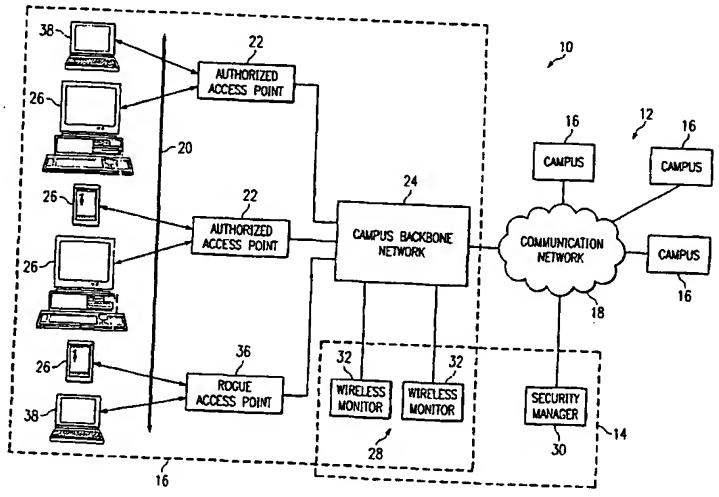
Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR REMOTELY MONITORING WIRLESS NETWORKS



(57) Abstract: A system for monitoring a wireless network is provided. The system includes a security network including a plurality of monitoring devices coupled to a centralized security manager. The security network is operable to manage access to a data network associated with a plurality of authorized devices. Each monitoring device is operable to receive packets communicated from one or more wireless device and communicate one or more of the packets to the centralized security manager. Each packet is associated with a communication session. The centralized security manager is operable to receive and analyze the one or more packets communicated from each monitoring device. The centralized security manager is further operable to determine whether a particular communication session is valid based on the analysis of at least one particular packet associated with a particular wireless device, and to communicate an alert if the particular communication session is not valid.

WO 2004/023730 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/27644

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	BAHL P ET AL: "PAWNS: SATISFYING THE NEED FOR UBIQUITOUS SECURE CONNECTIVITY AND LOCATION SERVICES" IEEE WIRELESS COMMUNICATIONS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 9, no. 1, February 2002 (2002-02), pages 40-48, XP001077105 ISSN: 1070-9916	1,2,4-7, 17-20, 22,23, 32-37, 39,40, 52,53
A	page 43, right-hand column, line 6 - page 44, right-hand column, line 13	41

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 July 2004	15/07/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Palencia Gutiérrez,C

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 03/27644

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002087882 A1	04-07-2002	AU 4735101 A	03-10-2001
		WO 0171499 A1	27-09-2001
US 2002036991 A1	28-03-2002	JP 2002111870 A	12-04-2002
US 2002094777 A1	18-07-2002	NONE	
WO 9638994 A	05-12-1996	GB 2301751 A	11-12-1996
		AU 2245799 A	20-05-1999
		AU 2245899 A	27-05-1999
		AU 710839 B2	30-09-1999
		AU 5972896 A	18-12-1996
		AU 5973296 A	18-12-1996
		AU 5973396 A	18-12-1996
		AU 5973796 A	18-12-1996
		AU 5973896 A	24-12-1996
		AU 5974896 A	18-12-1996
		AU 5975096 A	18-12-1996
		AU 5975896 A	18-12-1996
		AU 5977896 A	18-12-1996
		AU 5984896 A	18-12-1996
		AU 5985396 A	18-12-1996
		AU 6032896 A	18-12-1996
		AU 6033896 A	18-12-1996
		AU 6034896 A	18-12-1996
		AU 6034996 A	18-12-1996
		AU 6037696 A	18-12-1996
		AU 6037796 A	18-12-1996
		AU 6044296 A	18-12-1996
		AU 6148996 A	18-12-1996
		AU 705738 B2	03-06-1999
		AU 6475896 A	18-12-1996
		BR 9608335 A	05-01-1999
		BR 9608346 A	05-01-1999
		BR 9608347 A	05-01-1999
		BR 9608656 A	18-05-1999
		BR 9609300 A	15-06-1999
		BR 9609468 A	02-03-1999
		CA 2222705 A1	05-12-1996
		CA 2222734 A1	05-12-1996
		CN 1194071 A	23-09-1998
		CN 1191045 A	19-08-1998
		CN 1192831 A	09-09-1998
		DE 69601795 D1	22-04-1999
		DE 69604584 D1	11-11-1999
		DE 69606710 D1	23-03-2000
		DE 69606710 T2	31-08-2000
		DE 69609867 D1	21-09-2000
		DE 69609968 D1	28-09-2000
		DE 69623013 D1	19-09-2002
		DE 69623013 T2	12-12-2002
		DE 69623774 D1	24-10-2002
		DE 69623774 T2	15-05-2003
		DE 69624110 D1	07-11-2002
		DE 69624110 T2	22-05-2003
		DE 69629465 D1	18-09-2003
		DE 69629465 T2	01-07-2004